InViz: Instant Visualization of Security Attacks

Lucas Layman, Nico Zazworka
Fraunhofer Center for Experimental Software Engineering
College Park, MD, USA
{llayman,nzazworka}@fc-md.umd.edu

***Abstract*— The InViz tool is a functional prototype that provides graphical visualizations of network cybersecurity events to support real-time cyber forensics. Through visualization, both experts and novices in cybersecurity can analyze patterns of network behavior and investigate potential cybersecurity attacks. The goal of this research is to identify and evaluate the cybersecurity information to visualize that reduces the amount of time required to perform cyber forensics.**

Cybersecurity; visualization; real-time forensics; cyber forensics

I. Challenges in Attack Monitoring & Forensics

Network cybersecurity attacks take on many forms, from network breaches to denial-of-service attacks to insider threats exfiltrating sensitive data. A study by Verizon and the U.S. Secret Service found that 98% of data theft took place on network servers, and that 86% of victims had evidence of the breach in their log files [1]. Despite the presence of such evidence, most victims did not find the evidence of a breach until it is too late (see Figure 1).

The lag time between attack, detection and containment can be attributed to shortcomings in automated cyber defense systems and the challenges facing human users in investigating cyberattacks. The volume of network and log file information available has necessitated automated analysis solutions for detecting cybersecurity attacks. These automated systems are useful for processing large amounts of esoteric information, but, like many predictive systems, generate a high number of false positives in addition to missing attacks. In any case, a human agent (e.g. an IT administrator) must often step in to perform cyber forensics – verify the attack, identify its origin, determine any losses, and take corrective action. The tools to support cyber forensics are often primitive, often no more sophisticated than a text editor or Microsoft Excel [3]. Much current cybersecurity research focuses on automated detection of anomalous events or defensive practices, often ignoring how to support the humans performing cyber forensics.

II. Visualization to Support Human Cyber Forensics & Monitoring

The objective of this research is to identify, define, and evaluate the graphical information that is most useful for performing network cyber forensics in real-time. Just as researchers investigate what information to show in an aircraft controller's display, fundamental research is needed to identify the ideal information display for a security expert (or novice) monitoring and investigating a potential security attack. Most current visualization techniques are limited to statistical charts, such as line charts, bar charts and the like. These representations are one- or two-dimensional and are thus limited in the scope of information they can represent at any one time. Multi-dimensional information is required for a person (or automated agent, for that matter) to verify an attack in real-time.

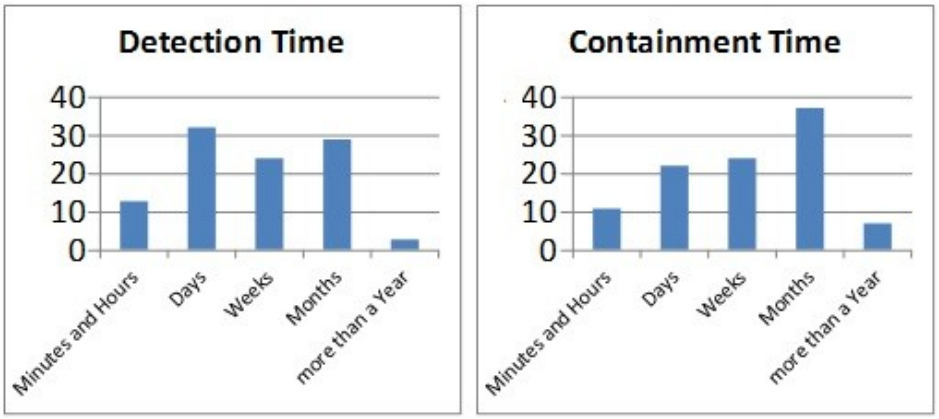

Figure 1. Times to detect and contain a security attack [1]

We have identified cybersecurity visualization concepts that may improve the efficacy of cyber forensics. To illustrate our cybersecurity visualization concepts, Fraunhofer CESE has created an initial research prototype called InViz – Instant Visualization of cybersecurity attacks (see Figure 2). These InViz cybersecurity visualizations combine concepts from glTail [4] and CodeVizard [5] to distill large amounts of information into a form more easily palatable to the user. These visualizations leverage the human capacity for pattern recognition to identify anomalous events. By being able to process this information quickly, humans can also apply their contextual knowledge of the system to eliminate false positives, thus reducing the time to perform rapid/live forensics. The real-time information visualization fills an important gap in the current cyber forensics marketplace and is a scientific contribution to "usable security" – one of the U.S. Department of Homeland Security's "Hard Problems in INFOSEC Research" [2].

REFERENCES

[1] Verizon, "2010 Data Breach Investigations Report", http://www.verizonbusiness.com/resources/reports/rp_2010-DBIR-combined-reports_en_xg.pdf, 2010.

[2] U.S. Department of Homeland Security, "A Roadmap for Cybersecurity Research", http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf, 2009, pp. 90-98.

[3] G.A. Fink, C.L. Noth, A. Endert, S. Rose, "Visualizing cyber security: Usable workspaces", 6th IEEE International Workshop on Visualization for Cyber Security (VizSec '09), Atlantic City, New Jersey, October 11 2009, pp. 45-56.

[4] "glTail.rb – realtime logfile visualization", http://www.fudgie.org, 2007.

[5] N. Zazworka, C. Ackermann, "CodeVizard: a tool to aid the analysis of software evolution", 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM '10), Bolzano-Bozen, Italy, Sept. 16-17 2010

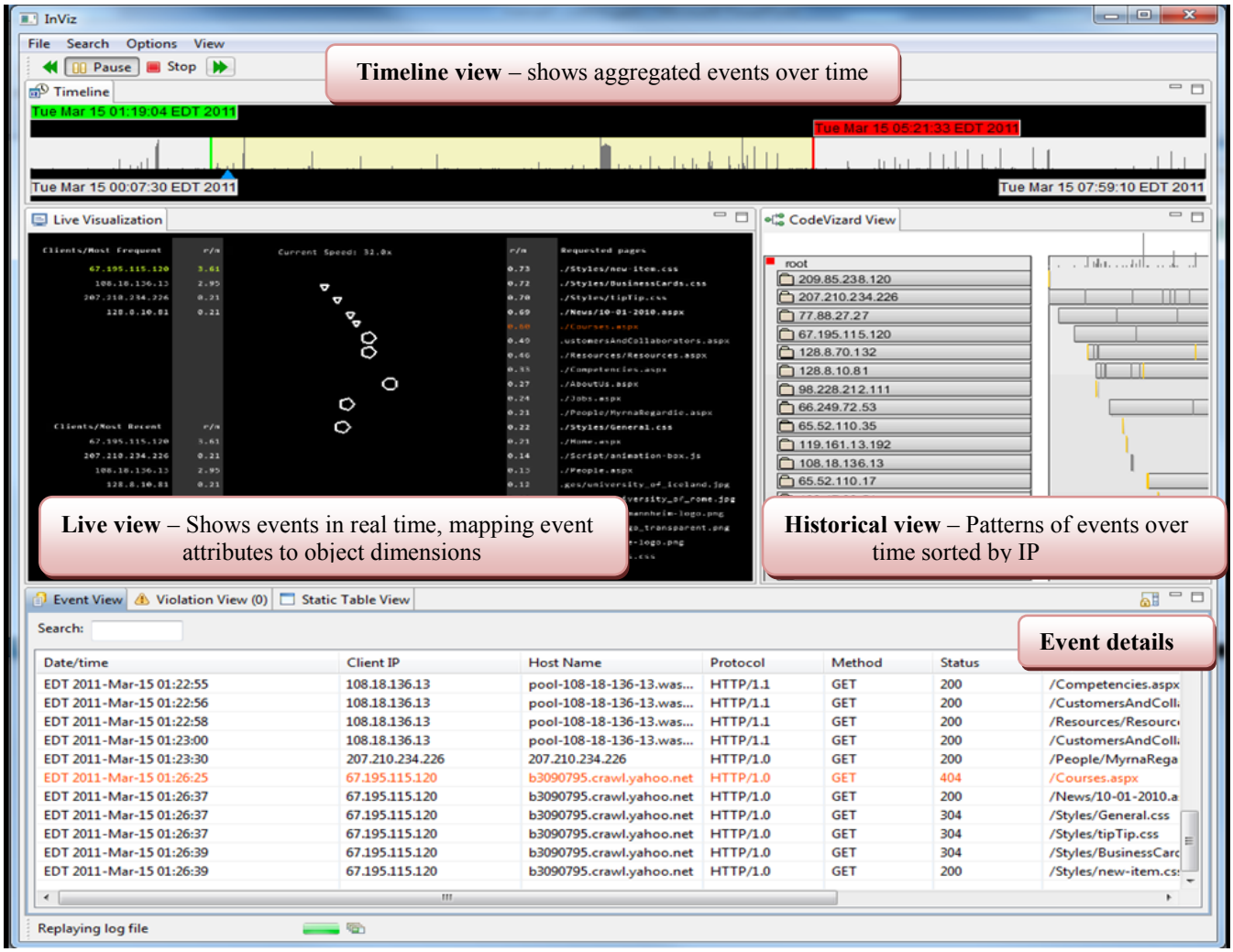

Figure 2. Screenshot of the InViz prototype processing IIS 7.5 webserver events